UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/727,953	11/30/2000	Guy McIlroy	PALM-3281.US.P	5875

49637 7590 08/31/2010

BERRY & ASSOCIATES P.C.
9229 SUNSET BOULEVARD
SUITE 630
LOS ANGELES, CA 90069

EXAMINER	
KHOSHNOODI, NADIA	
ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
08/31/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/727,953	MCILROY, GUY	
	Examiner	Art Unit	
	NADIA KHOSHNOODI	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 July 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 4-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 4-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 May 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 7/9/2010 has been entered.

Response to Amendment

Claims 2-3 and 22-28 have been cancelled. Applicant's arguments/amendments with respect to the pending claims filed 7/9/2010 have been fully considered but are moot in view of new grounds rejection.

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 1, 4-5, 8-13, 15-18, and 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wentker et al., US Patent No. 6,481,632 and further in view of Muttik et al., US Patent No. 6,907,396.

As per claim 1:

Wentker et al. substantially teach a method of ensuring the security of an open platform computer system, comprising loading software suitable for operating on an open platform computer system in a secure environment on the open platform computer system comprising the host facility and the portable computing device (col. 4, lines 43-63 and col. 12, lines 9-21); upon loading the software on the open platform computer system, initiating a pre-synchronization scan (col. 12, lines 49-57); during a pre-synchronization scan, validating the software by the use of a validator program residing in the open platform computer system in a secure fashion such that the validator program scans the software that is loaded in a secure environment (col. 15, lines 8-19); marking the software as valid or invalid by the use of a flag (col. 15, lines 15-19); and, automatically denying the software the ability to operate on any environment within the computer system and denying synchronization of the software with the portable computer device if the validator fails to identify the software as valid in order to ensure the security of the open platform computer system (col. 9, lines 34-65 and col. 10, lines 31-39).

Not explicitly disclosed is wherein the act of scanning and validating comprises running the code in an emulator for the open platform computer system within the secure environment comprising a modified operating system for the emulator to run in, allowing the execution of the code to be examined for any new malicious routines as well as against known malicious signatures. However Muttik et al. teach using an emulator to run code in order to analyze the code to determine if any malicious routines or known malicious signatures are found (col. 4, lines 4-23). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wentker et al. to scan the software in an emulator to discover any malicious routines or known malicious signatures that may be present in the

code. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Muttik et al. suggest that emulating the code in a protected region first prevents the code from damaging a computer system in col. 4, lines 15-23.

As per claim 4:

Wentker et al. and Muttik et al. substantially teach the method described in claim 1. Furthermore, Wentker et al. teach wherein said software is supplied by a third-party source (col. 13, lines 40-60).

As per claim 5:

Wentker et al. and Muttik et al. substantially teach the method described in claim 4. Furthermore, Wentker et al. teach wherein said third-party software is for execution or other use on a palmtop computer (col. 4, lines 43-63).

As per claim 8:

Wentker et al. substantially teach a method of ensuring the security of an open platform computer system, comprising a validations program residing on the open platform computer system in a secure fashion that is configured for: a portable computing device coupled to a host computer, wherein the portable computing device is configured to load software from the host computer to the portable computing device for operating on the portable computing device (col. 12, lines 9-21); a validation program residing on the open platform computer system in a secure fashion (col. 12, lines 49-57) that is configured for: validating the software during a pre-synchronization scan by first scanning the software that is loaded in a secure environment (col. 15, lines 8-19); marking the software as valid or invalid by the use of a flag (col. 15, lines 15-

19); and, automatically denying the software the ability to operate on any environment within the computer system and denying synchronization of the software with the portable computing device if the validator fails to identify the software as valid in order to ensure the security of said computer system (col. 9, lines 34-65 and col. 10, lines 31-39).

Not explicitly disclosed is wherein the act of scanning and validating comprises running the code in an emulator for the open platform computer system within the secure environment comprising a modified operating system for the emulator to run in, allowing the execution of the code to be examined for any new malicious routines as well as against known malicious signatures. However Muttik et al. teach using an emulator to run code in order to analyze the code to determine if any malicious routines or known malicious signatures are found (col. 4, lines 4-23). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wentker et al. to scan the software in an emulator to discover any malicious routines or known malicious signatures that may be present in the code. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Muttik et al. suggest that emulating the code in a protected region first prevents the code from damaging a computer system in col. 4, lines 15-23.

As per claim 9:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 8. Furthermore, Muttik et al. teach wherein said host computer is coupled to a network (col. 3, lines 54-62).

As per claim 10:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 8. Furthermore, Wentker et al. teach wherein the portable computing device is a handheld computing device (col. 4, lines 43-63).

As per claim 11:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 8. Furthermore, Wentker et al. teach wherein the portable computing device is a personal data assistant (col. 4, lines 43-63).

As per claim 12:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 8. Furthermore, Wentker et al. teach wherein the portable computing device is coupled to said host computer by an infrared device (col. 5, lines 28-40).

As per claim 13:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 8. Furthermore, Wentker et al. teach wherein the portable computing device is coupled to said host computer by an RF enabled device (col. 5, lines 28-40).

As per claim 15:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 8. Wentker et al. further teach wherein said validation program is configured to evaluate third-party software and attach a digital "valid" flag if the third-party software is found to be clean of known security compromising routines or attach a digital "invalid" flag to the third-party software if the third-party software is not found to be clean of known security compromising routines (col. 12,

line 58 – col. 13, line 10 and col. 15, lines 1-19).

As per claim 16:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 15. Wentker et al. further teach wherein said portable computing device is configured to load third-party software files with the digital "valid" flag attached and to refrain from loading third-party software files which have no flag attached or have the "invalid" flag attached (col. 15, lines 1-51).

As per claim 17:

Wentker et al. and Muttik et al. substantially teach the apparatus described claim 15. Furthermore, Wentker et al. teach wherein said portable computing device is a personal data assistant (col. 4, lines 43-63).

As per claim 18:

Wentker et al. substantially teach an apparatus of ensuring the security of an open platform computer system, comprising a validations program residing on the network that is configured for: a handheld computing device coupled to a network, wherein the handheld computing device is configured to load software from the network to the handheld computing device for operation on the handheld computing device (col. 4, lines 43-63 and col. 12, lines 9-21); validating the software by scanning files of the software in a secure environment on the handheld computing device upon loading the software in any environment on the handheld computing device (col. 12, lines 49-57); marking the software as valid or invalid by the use of a flag (col. 15, lines 15-19); and, automatically denying the software the ability to operate on any

environment within the computer system if the validator fails to identify the software as valid in order to ensure the security of said computer system (col. 9, lines 34-65 and col. 10, lines 31-39).

Not explicitly disclosed is wherein the act of scanning and validating comprises running the code in an emulator for the open platform computer system within the secure environment comprising a modified operating system for the emulator to run in, allowing the execution of the code to be examined for any new malicious routines as well as against known malicious signatures. However Muttik et al. teach using an emulator to run code in order to analyze the code to determine if any malicious routines or known malicious signatures are found (col. 4, lines 4-23). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wentker et al. to scan the software in an emulator to discover any malicious routines or known malicious signatures that may be present in the code. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Muttik et al. suggest that emulating the code in a protected region first prevents the code from damaging a computer system in col. 4, lines 15-23.

As per claim 20:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 18. Wentker et al. further teach wherein said portable computing device is configured to load third-party software files with the digital "valid" flag attached and to refrain from loading third-party software files which have no flag attached or have the "invalid" flag attached (col. 15, lines 1-51).

As per claim 21:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 18. Wentker et al. further teach wherein said validation program is configured to evaluate third-party software and attach a digital "valid" flag if the third-party software is found to be clean of known security compromising routines or attach a digital "invalid" flag to the third-party software if the third-party software is not found to be clean of known security compromising routines (col. 12, line 58 – col. 13, line 10 and col. 15, lines 1-19)

III. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wentker et al., US Patent No. 6,481,632 and Muttik et al., US Patent No. 6,907,396, as applied to claim 1 above, and further in view of Brody, US Pub. No. 2001/0051928.

As per claim 7:

Wentker et al. and Muttik et al. substantially teach the method described in claim 1. Muttik et al. also teach a host computer (col. 3, lines 54-62). Furthermore, Muttik et al. teach that the computing environment allows for various computing systems, one of which may be a personal organizer (col. 3, lines 44-49). Not explicitly disclosed is wherein said method operates on a computer system which comprises a portable computing device coupled to said host computer and wherein the validating operation is performed by the host computer for the portable computing device. However, Brody teaches a PDA coupled to a host device for personalization purposes. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wentker et al. to have the hand-held device coupled to the host computer in order to carry out different functions on the palmtop computing device. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so

since Brody suggests that PDA's are used in conjunction with PC's in order to download applications because PDA's are highly mobile and the client can always have access to his/her PDA in par. 33, lines 1-30.

IV. Claims 6, 14, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wentker et al., US Patent No. 6,481,632 and Muttik et al., US Patent No. 6,907,396, as applied to claims 1, 8, & 18 above, and further in view of Ginter et al., US Patent No. 6,948,070.

As per claim 6:

Wentker et al. and Muttik et al. substantially teach the method described in claim 1. Not explicitly disclosed is wherein said validator program is specially constructed to reside in a secure fashion in the host facility of said computer system. However, Ginter et al. teach the use of a tamper-resistant security barrier which could be included in any component in a network so that processes are ensured to be carried out within a secure environment. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wentker et al. for the validator program to be contained within a secure environment in order to ensure that it has not been tampered with so that it correctly validates the software/application. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ginter et al. suggest that it is important to ensure that processes are carried out within a secure environment in col. 59, lines 48-59.

As per claim 14:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 8. Not explicitly disclosed is wherein said validation program resides in said host computer of the

computer system in a fashion intended to be secure. However, Ginter et al. teach the use of a tamper-resistant security barrier which could be included in any component in a network so that processes are ensured to be carried out within a secure environment. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the apparatus disclosed in Wentker et al. for the validator program to be contained within a secure environment in order to ensure that it has not been tampered with so that it correctly validates the software/application. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ginter et al. suggest that it is important to ensure that processes are carried out within a secure environment in col. 59, lines 48-59.

As per claim 19:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 18. Not explicitly disclosed is wherein said validation program resides in said computer network in a fashion intended to be secure. However, Ginter et al. teach the use of a tamper-resistant security barrier which could be included in any component in a network so that processes are ensured to be carried out within a secure environment. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the apparatus disclosed in Wentker et al. for the validator program to be contained within a secure environment in order to ensure that it has not been tampered with so that it correctly validates the software/application. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ginter et al. suggest that it is

important to ensure that processes are carried out within a secure environment in col. 59, lines 48-59.

**References Cited, Not Used*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. US Patent No. 6,694,436
2. US Patent No. 5,953,502
3. US Patent No. 7,080,407
4. US Patent No. 6,981,279
5. US Patent No. 6,481,632 – cited in reference to an "open platform" architecture/system
6. US Patent No. 7,243,236
7. US Pub. No. 2002/0069263

The above references have been cited because they are relevant due to the manner in which the invention has been claimed.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nadia Khoshnoodi/
Examiner, Art Unit 2437
8/25/2010

NK

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437